

CLAIMS

1. A denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system

5 comprising:

a monitoring device that monitors a packet transmitted to a communication device that is a target of the denial-of-service attack;

a performance measuring device that measures
10 performance of the communication device; and

an attack determining device that performs communication with the monitoring device and the performance measuring device, wherein

the monitoring device includes a traffic abnormality
15 detecting unit that detects traffic abnormality information indicating an abnormality of traffic due to the packet with respect to the communication device,

the performance measuring device includes a performance abnormality detecting unit that detects
20 performance abnormality information indicating an abnormality of throughput of the communication device, and

the attack determining device includes an effects determining unit that determines whether the communication device received the denial-of-service attack, based on the
25 traffic abnormality information and the performance abnormality information.

2. The denial-of-service attack detecting system according to claim 1, wherein

30 the monitoring device further includes a traffic-abnormality-information transmitting unit that transmits the traffic abnormality information to the attack determining device.

3. The denial-of-service attack detecting system according to claim 1 or 2, wherein

the performance measuring device further includes a performance-abnormality-information transmitting unit that transmits the performance abnormality information to the attack determining device.

4. The denial-of-service attack detecting system according to claim 1, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a predetermined attack detection condition that is set in advance.

5. The denial-of-service attack detecting system according to claim 4, wherein

the traffic abnormality detecting unit generates a signature indicating a feature of the packet attacking the communication device, based on the attack detection condition, and generates the traffic abnormality information including the signature.

6. The denial-of-service attack detecting system according to claim 1, wherein

the traffic abnormality detecting unit detects the traffic abnormality information based on a steady traffic indicating an average traffic of the packet transmitted to the communication device.

7. The denial-of-service attack detecting system according to claim 1, wherein

the performance abnormality detecting unit detects the performance abnormality information based on a

predetermined performance abnormality detection condition that is set in advance.

8. The denial-of-service attack detecting system
5 according to claim 7, wherein
the performance abnormality detection condition includes

a response time from transmission of a response
request message to the communication device to reception of
10 a response message corresponding to the response request
message; and

number of times that the response time exceeds a
predetermined threshold.

15 9. The denial-of-service attack detecting system
according to claim 1, wherein
the performance abnormality detecting unit detects the
performance abnormality information based on a steady
performance indicating an average performance feature of
20 the communication device.

10. The denial-of-service attack detecting system
according to claim 1, wherein
the effects determining unit determines that the
25 communication device received the denial-of-service attack,
when it is determined that one of the traffic abnormality
information and the performance abnormality information
causes an occurrence of other of the traffic abnormality
information and the performance abnormality information
30 based on an abnormality occurrence time included in the
traffic abnormality information and the performance
abnormality information.

11. The denial-of-service attack detecting system according to claim 1, wherein

when the effects determining unit determines that the communication device received the denial-of-service attack,
5 the attack determining device transmits the traffic abnormality information and the performance abnormality information used for the determination to a device for reporting to an operator.

10 12. The denial-of-service attack detecting system according to claim 1, wherein

the effects determining unit determines whether the communication device received the denial-of-service attack, after performing an authorization based on certificates
15 included in the traffic abnormality information and the performance abnormality information.

13. A method of detecting a denial-of-service attack on a communication device by using a monitoring device that
20 monitors a packet transmitted to a communication device that is a target of the denial-of-service attack, a performance measuring device that measures performance of the communication device, and an attack determining device that performs communication with the monitoring device and
25 the performance measuring device, the method comprising:

traffic abnormality detecting including the monitoring device detecting traffic abnormality information indicating an abnormality of traffic due to the packet with respect to the communication device;

30 performance abnormality information detecting including the performance measuring device detecting performance abnormality information indicating an abnormality of throughput of the communication device; and

effects determining including the attack determining
device determining whether the communication device
received the denial-of-service attack, based on the traffic
abnormality information and the performance abnormality
5 information.

14. The method according to claim 13, further comprising:
traffic abnormality information transmitting including
the monitoring device transmitting the traffic abnormality
10 information to the attack determining device.

15. The method according to claim 13 or 14, further
comprising:
performance abnormality information transmitting
15 including the performance measuring device transmitting the
performance abnormality information to the attack
determining device.